

CLAIMS

What is claimed is:

1 1. A method for booting up a computer system in a secure fashion comprising the steps
2 of:

3 a) determining the presence of a security feature element during an initialization
4 of the computer system wherein the security feature element includes a public key and a
5 corresponding private key;

6 b) storing a portion of the public key in a nonvolatile memory within the
7 computer system if the security feature element is present; and

8 c) utilizing an algorithm to determine the presence of the security feature
9 element prior to a subsequent boot-up of the computer system.

1 2. The method of claim 1 wherein the security feature element comprises a security
2 card.

1 3. The method of claim 2 wherein the security card provides for tamper detection of the
2 computer system and the security card, temperature monitoring of the computer system and
3 voltage status reporting of the computer system.

1 4. The method of claim 1 wherein step c) is performed during a Power-On-Self-Test
2 (POST) sequence.

1 5. The method of claim 4 wherein step c) further comprises:

2 c1) determining the presence of the security card.

1 6. The method of claim 5 wherein step c1) further comprises:

2 c1a) determining if the computer system has been subjected to a tamper event if
3 the security card is present.

1 7. The method of claim 6 wherein step c1) further comprises:

2 c1a) determining whether a security card was previously present in the computer
3 system if the security card is not present.

1 8. The method of claim 7 wherein step c1) further comprises:

2 c1b) clearing the portion of the public key stored in the non-volatile memory of
3 the computer system if a security card was previously present in the computer system; and

4 c1c) prompting for an authorization prior to booting up the computer system.

1 9. The method of claim 7 wherein step c1) further comprises:

2 c1b) booting up the computer system if the security card was not previously
3 present in the computer system.

1 10. The method of claim 6 wherein step c1) further comprises:

2 c1b) booting up the computer system if the computer system has not been
3 subjected to a tamper event.

1 11. The method of claim 6 wherein step c1) further comprises:

2 c1b) determining whether the security card is an added feature of the computer
3 system, wherein the determination is based on a previous POST sequence, if the computer
4 system has been subjected to a tamper event.

1 12. The method of claim 11 wherein step c1) further comprises:

2 c1c) clearing the portion of the public key stored in the nonvolatile memory of the
3 computer system if the card is a newly added feature of the computer system; and

4 c1d) prompting for an authorization prior to booting up the computer system.

1 13. The method of claim 11 wherein step c1) further comprises:

2 c1c) comparing the public key on the security card with the portion of the public
3 key stored in the nonvolatile memory of the computer system if the security card is not a
4 newly added feature of the computer system.

1 14. The method of claim 13 wherein step c1) further comprises:

2 c1d) booting up the computer system if the public key on the security card
3 matches the portion of the public key stored in the nonvolatile memory of the computer
4 system.

1 15. The method of claim 13 wherein step c1) further comprises:

2 c1d) clearing the portion of the public key stored in the nonvolatile memory of the
3 computer system;

4 cle) clearing the public key and the corresponding private key stored on the
5 security card; and

6 clf) booting up the computer system.

1 16. A system for booting up a computer in a secure fashion, the system comprising:

2 means for determining the presence of a security feature element during an
3 initialization of the computer system wherein the security feature element includes a public
4 key and a corresponding private key;

5 means for storing a portion of the public key in a nonvolatile memory within the
6 computer system if the security feature element is present; and

7 means for utilizing an algorithm to determine the presence of the security feature
8 element prior to a subsequent boot-up of the computer system.

1 17. The system of claim 16 wherein the security feature element comprises a security
2 card.

1 18. The system of claim 17 wherein the security card provides for tamper detection of
2 the computer and the security card, temperature monitoring of the computer and voltage
3 status reporting of the computer.

1 19. The system of claim 18 wherein the algorithm is utilized during a Power-On-Self-
2 Test (POST) sequence.

1 20. The system of claim 19 wherein the means for utilizing the algorithm further
2 comprises:

3 means for determining the presence of the security card.

1 21. The system of claim 20 wherein the means for utilizing the algorithm further
2 comprises:

3 means for determining if the computer has been subjected to a tamper event if the
4 security card is present.

1 22. The system of claim 20 wherein means for utilizing the algorithm further comprises:
2 means for determining whether a security card was previously present in the
3 computer if the security card is not present.

1 23. The system of claim 22 wherein the means for determining the presence of the
2 security card further comprises:

3 means for clearing the portion of the public key stored in the non-volatile memory of
4 the computer if a security card was previously present in the computer; and

5 means for prompting for an authorization prior to booting up the computer.

1 24. The system of claim 22 wherein the means for determining the presence of the
2 security card further comprises:

3 means for booting up the security system if the security card was not previously
4 present in the computer.

1 25. The system of claim 21 wherein the means for determining the presence of the
2 security card further comprises:

3 means for booting up the computer if the computer has not been subjected to a
4 tamper event.

1 26. The system of claim 21 wherein the means for determining the presence of the
2 security card further comprises:

3 means for determining whether the card is a newly added feature of the computer,
4 wherein the determination is based on a previous POST sequence, if the computer has been
5 subjected to a tamper event.

1 27. The system of claim 26 wherein the means for determining the presence of the
2 security card further comprises:

3 means for clearing the portion of the public key stored in the nonvolatile memory of
4 the computer if the card is a newly added feature of the computer; and

5 means for prompting for an authorization prior to booting up the computer.

1 28. The system of claim 26 wherein the means for determining the presence of the
2 security card further comprises:

3 means for comparing the public key on the security card with the portion of public
4 key stored in the nonvolatile memory of the computer if the security card is not a newly
5 added feature of the computer.

1 29. The system of claim 28 wherein the means for determining the presence of the
2 security card further comprises:

3 means for booting up the computer system if the public key on the security card
4 matches the portion of the public key stored in the nonvolatile memory of the computer.

1 30. The system of claim 28 wherein the means for determining the presence of the
2 security card further comprises:

3 means for clearing the portion of the public key stored in the nonvolatile memory of
4 the computer;

5 means for clearing the public key and the corresponding private key stored on the
6 security card; and

7 means for prompting for an authorization prior to booting up the computer.